VENABLE LLP

HOW SAILPOINT'S CAPABILITIES ADDRESS THE NIST CYBERSECURITY FRAMEWORK

Introduction

In today's complex enterprise environments, understanding how technology can enable the successful management of risk is essential. There is no one tool that can protect the assets of an entire organization, but knowing what tools are needed and where to deploy them can be daunting, even to well-resourced organizations. Over the years, frameworks have emerged to aid in this process of identifying gaps and the associated people, processes and technology approaches that can help to close them.

One relatively recent and highly successful framework is the NIST Cybersecurity Framework ("Framework" or "CSF"). The CSF covers a wide range of capabilities in recognition of the fact that all organizations will be under different threats, have different levels of resources at their disposal, and be at different places in their development and implementation of cybersecurity risk management. Understanding how any given capability or tool will help organizations more effectively use the Framework is critical to building a robust and measurable cybersecurity program, regardless of sector or industry.

One key area of that risk management is Identity and Access Management and the CSF enumerates a number of capabilities that enable enterprises to effectively understand and manage identity governance across their organization.

Specifically, this paper examines how the SailPoint Governance Platform addresses these capabilities and our analysis shows that implementing SailPoint's capabilities will assist organizations in addressing 35 of the 108 Subcategories in the NIST Framework, in whole or in part.

As noted earlier, no tool can or should be expected to meet all 108 of the NIST CSF Subcategories. SailPoint's capabilities are useful as part of a comprehensive cybersecurity risk management program when used in conjunction with other tools. Correspondingly, SailPoint has built a large number of partnerships with vendors of other capabilities that when combined, create robust risk management systems. For the purposes of our analysis, we only considered SailPoint's capabilities on their own.

Unsurprisingly, the SailPoint Governance Platform does exceptionally well in those Framework Subcategories tied directly and indirectly to identity and access management, of which there are several. However, we also found that because of the foundational nature of identity and access management, SailPoint's Governance Platform also brings capabilities that can enhance other technologies and processes.

Appendix A provides additional detail on the NIST Cybersecurity Framework and the matrix in Appendix B offers a detailed assessment of all NIST Subcategories that can be addressed by SailPoint capabilities.

Methodology

In conducting our analysis, we systematically reviewed the documentation and the demonstrated feature set of all SailPoint solutions. We interviewed lead engineers at SailPoint, and gained a firm understanding of the product capabilities and how they are typically deployed.[1]

The NIST Framework can be used in a wide range of use cases, and its Functions, Categories, and Subcategories are designed to be context agnostic. To conduct a meaningful analysis, it is necessary to understand the context in which we view the SailPoint capabilities operating. To that end, we have made the following assumptions:

- The environment is a typical enterprise, with a mix of on-premises and cloud-based applications;
- All SailPoint solutions are implemented fully across all possible assets;
- Third-party providers/partners are granted appropriate levels of access to certain enterprise systems; and
- The enterprise cybersecurity program is generally mature and takes a defense-in-depth approach to managing risk.

Environments where these criteria are different may find that certain capabilities defined here may vary in completeness.

While each Subcategory in the CSF is presented largely as a "yes/no" interaction, in the real world, things are rarely that simple. To this end, we endeavor to be more specific in our assessment and recognize varying degrees of alignment, as some capabilities align to certain Subcategories more than others:

- COMPLETE: One or more SailPoint capabilities addresses all components of the NIST Subcategory in the defined context.
- CONTRIBUTE: One or more SailPoint capabilities assists in addressing the NIST Subcategory for the defined context.
- INFORM: Outputs of SailPoint capabilities enhance and provide insight into addressing the NIST Subcategory for the defined context.

Framework Subcategories not addressed by any SailPoint capability were omitted from this report.

Mapping SailPoint's Capabilities to the NIST Framework

The SailPoint Governance Platform is a collection of products that cover a wide range of capabilities, primarily focused around identity and access management. Combined, these products provide insight and control over what users do and should have access to, and how they are using that access. Importantly, because SailPoint can deeply integrate IT and business roles, the overall impact spans people, process and technology.

In our review, we identified three distinct capabilities that are useful when considering how these solutions fit within the context of the CSF:

[1] Venable did not operate the SailPoint solutions directly.

- Governance: Development, implementation and enforcement of identity related policies and provisioning actions;
- Access Control: Assign roles, manage authentication, and control access to data.
- Analytics: Behavioral analysis and machine-learning to see, audit and assess user activity and risk.

Note that these represent our view of what the solutions provide, and not necessarily how SailPoint my represent them. You can review our complete analysis in the attached matrix (Appendix B). As an overview, however, you can see that together, these capabilities address NIST Subcategories across four of the five NIST Functions:

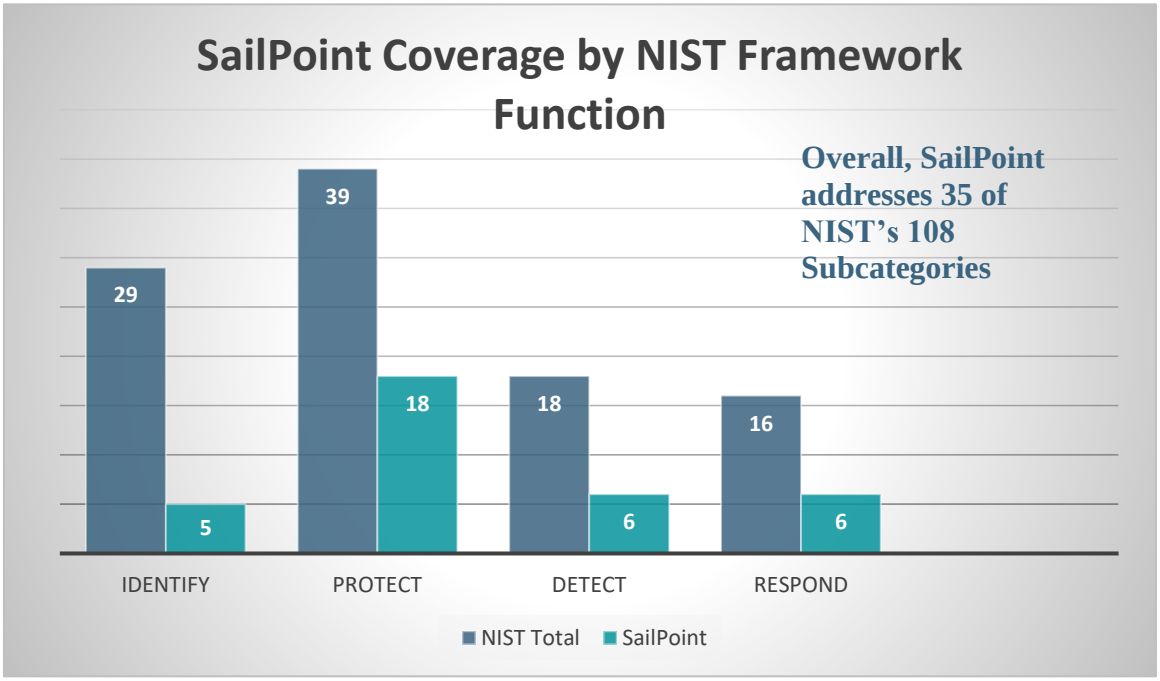

Figure 1: Coverage by NIST Framework Function

These 35 Subcategories are distributed across the three primary product capabilities as follows:

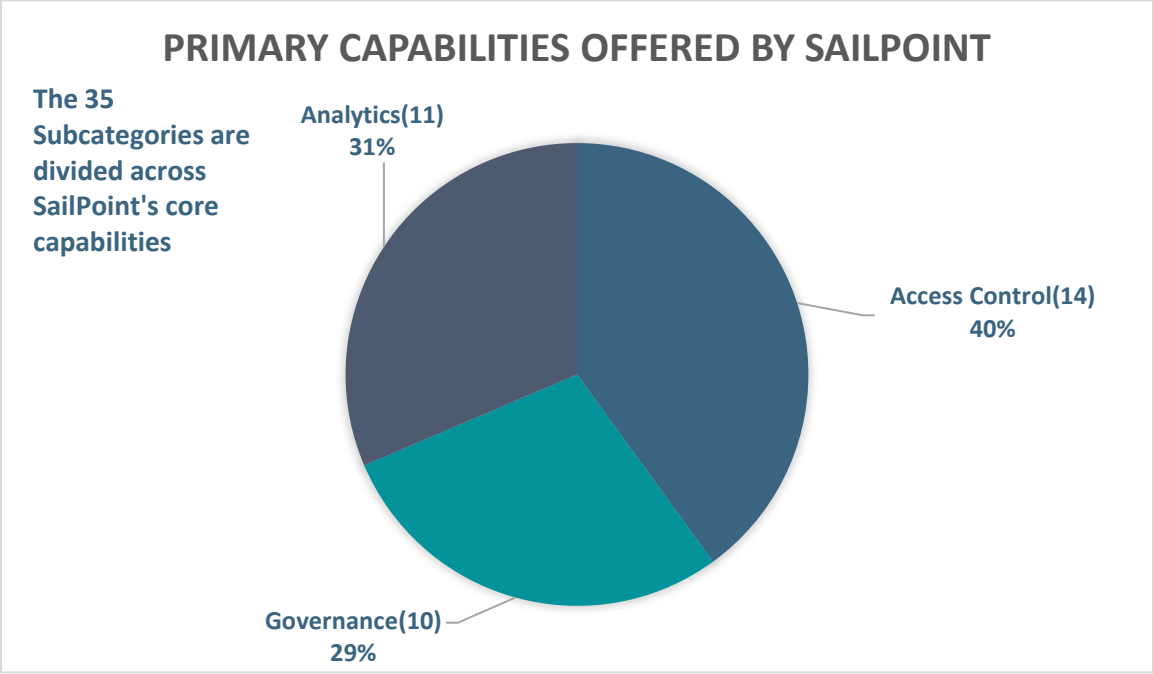

Figure 2: SailPoint Framework Coverage by product capability

It is important to recognize that the distribution of included Subcategories across Functions and capabilities as shown above is influenced by the distribution of all Subcategories within the CSF itself. As a result, what we see is not necessarily a full representation of the SailPoint solutions, but rather how they intersect with what the CSF delineates. Regardless, as both Figures 1 and 2 demonstrate, SailPoint's overall coverage across the CSF is significant. It is also important to note that the CSF does not assign any weighting or importance to the Subcategories by which to prioritize them. From a practical standpoint, this means that each individual organization has to decide the importance of the SailPoint capabilities within their environment.

To better understand how we arrived at our conclusions, we provide some examples below for each SailPoint capability and demonstrate how certain Subcategories align with them, for COMPLETE, CONTRIBUTE, and INFORM circumstances. Appendix B contains the complete set.

Governance

SailPoint generally positions themselves as an "Identity Governance" solution company, which they define as providing "…complete visibility into who is doing what, what kind of risk that represents, and allows you to take action. It links people, applications, data and devices to create an identity-enabled enterprise."[2] As a result, you might expect this capability to have a much stronger representation in terms of Subcategory coverage. However, as mentioned earlier, we are working with what the CSF provides and in general, its coverage of "governance" areas tends to be fairly high level, which is comprehensive but lacking in granularity. This in turn has led to Governance having the fewest number of application Subcategories, but does not suggest that it is the weakest area.

In fact, Governance can be viewed as the overarching approach, with both Access Control and Analytics contributing critical but supporting activities. This is reinforced by the fact that all of the Subcategories we selected from the Identify Function are all related to Governance.

[2] https://www.sailpoint.com/identity-management-solutions/?elqct=Website&elqchannel=OrganicDirect

COMPLETE

PR.AC-4: Access permissions and authorization are managed, incorporating the principles of least privilege and separation of duties.

Unsurprisingly, we find that PR.AC-4 is a COMPLETE match to SailPoint's capabilities. At first glance, it might be tempting to think that this would be better placed in Access Control given that is references "Access permissions." However, our experience in implementing the Framework has repeatedly demonstrated that the intent behind any given Subcategory isn't always immediately clear. In this case, we contrast PR.AC-4 with PR.AC-1 (discussed further below). We would argue that PR.AC-1 involves direct action that supports the "managed" criteria for PR.AC-4, while PR.AC-4 represents the implementation of conceptual design principles and policies. This is not to suggest that PR.AC-4 isn't actionable, but rather that there is a useful distinction when considering how you are managing and measuring your risk.

CONTRIBUTE

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

Here, the CONTRIBUTE rating is due to the fact that the Subcategory references both "users and systems". If it were only for "users" then we think we could have another COMPLETE, as SailPoint's ability to monitor and track user actions is excellent. This is a great example to highlight one of the things to watch out for when using the CSF. The end goal for this Subcategory is fairly clear: understand what is going on with your network so that you can detect and prevent anomalous behavior and activities. However, how you achieve that goal can be architecturally dependent, and can be different between users and systems.

INFORM

ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

As mentioned above, Governance is well represented in the CSF Identify Function. In this example, we are considering the fact that what SailPoint provides in terms of visibility into user identities, permissions, and actions, is highly informative to developing organizational policies and procedures and assigning and managing roles and responsibilities. However, ID.GV-2 is addressing the organizational process around aligning roles and responsibilities and the analysis that goes into making those determinations, as opposed to the technology solutions that are implemented to manage them. Due to that distinction, we consider this to be an INFORM.

Access Control

COMPLETE

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

This is probably the most straightforward and obvious Subcategory that SailPoint meets, although to be fair it doesn't fully represent all of SailPoint's capabilities. In fact, you could add "and files" to the end of the Subcategory and have an even closer match.

CONTRIBUTE

RS.MI-1: Incidents are contained.

SailPoint does not position any of their solutions as incident management tools. But as anyone who has done incident management can attest, you want to use any and all tools at your disposal to assess and contain damage. In certain types of incidents, that containment is going to involve locking users out of systems, files, or processes in a timely and controlled fashion. Although not referenced in this section, you will note in Appendix B that we also consider SailPoint solutions to have usefulness in forensic analysis.

Analytics

Data collected by SailPoint is focused on users and the access they have across enterprise assets.

Analytics has long been a critical underpinning of the SailPoint Governance Platform. The underlying data has been there within their products even as the ability for customers to take full advantage of it is an evolving area. Missing from this capability is any Subcategory at the COMPLETE level. The reason for this is straightforward: enterprise analytics requires more than just data on users, meaning that SailPoint can't, nor is intended to, provide a full analytics solution.

CONTRIBUTE

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.

At first glance, it would be reasonable to assume that this Subcategory should be a COMPLETE. After all, SailPoint is focused on users and what they are doing. However, the one limiting factor is that users can potentially engage in activities after being authenticated, and those activities would not necessarily be captured by SailPoint. Instead, it would require other types of network and system monitoring technologies. Regardless, it's clear that SailPoint can play an important role in meeting this Subcategory.

INFORM

PR.IP-8: Effectiveness of protection technologies is shared.

We choose this Subcategory to represent an important concept we think SailPoint brings to the table in several areas. Given that identity governance is foundational to any well-managed enterprise, understanding how users interact across the organization can provide insights in important ways. For example, if you are segmenting networks in order to prevent different departments from accessing each other's systems, a properly implemented SailPoint solution can indicate whether any users are bypassing that segmentation. This can provide insight on possible gaps in implementations that are creating a security risk, or demonstrate that there are business requirements not previously understood or addressed.

Conclusion

Our analysis of SailPoint's capabilities is designed to provide cybersecurity decision makers and implementers with the knowledge necessary to best use the product's features and capabilities in an environment where the NIST Cybersecurity Framework is central to the overall risk management of the organization.

No one product is capable to achieving the full risk management approach that is needed to provide comprehensive defense and management of an enterprise. Organizations must bring together the right people, processes, and technologies, in the right way, to achieve that goal. Using the NIST Cybersecurity Framework is a useful and widely accepted means for assessing and measuring risk.

When implementing SailPoint in your enterprise, this analysis can assist in better understanding where and how the capabilities it provides align, and don't align with the Framework. Armed with that knowledge, gaps can be more effectively filled and managed over time.

APPENDIX A: UNDERSTANDING THE NIST CYBERSECURITY FRAMEWORK

The History of the Framework

Despite the attention being paid to cybersecurity in recent years, the risk isn't new. Organizations have been facing the threat of malicious actors using the Internet to commit all manner of espionage and crime for decades. However, as dependency on the Internet has grown, so too has the threat. Today, few organizations can conduct their business or achieve their mission without using the Internet; and as a result, malicious actors have grown in sophistication and determination. The amount of data available to steal is simply too attractive to ignore. So too is the ability to exert social and political impact anonymously or from the relative safety of thousands of miles away. The success of these actors has led to a seemingly endless stream of major data breaches, DDoS attacks, and other cyber-based nefarious activity. As a result, cybersecurity risk has slowly but surely moved from the purview of the enterprise information technology team, through the C-suite, and straight to the Board of Directors.

Understanding and mitigating these risks requires not only technical expertise, but the means to build a cybersecurity program that leverages the best thinking across the industry and enables communication of complex topics throughout an organization.

In 2013, and in response to increasing threats against the United States and its critical infrastructure, President Barack Obama issued Executive Order 13636 *Improving Critical Infrastructure Cybersecurity*, which among other things, directed the National Institute of Standards and Technology ("NIST") to produce a framework that could be used to understand and mitigate threats to critical infrastructure. The resulting document, formally titled *Framework for Improving Critical Infrastructure Cybersecurity*, was released in 2014, following a year of robust and inclusive meetings between hundreds of public and private sector stakeholders and experts.

Since its release, the NIST Cybersecurity Framework ("CSF" or "Framework") has seen remarkable adoption across all sectors, not just those identified as critical infrastructure. Its success can be directly attributed to a handful of factors:

- It is comprehensive in terms of coverage of security controls;
- It is written in relatively concise language making it accessible to many parts of an organization;
- It is traceable to multiple international standards and best practice guidelines; and
- It is flexible and non-prescriptive.

In May of 2016, the President of the United States issued an Executive Order entitled *Strengthening The Cybersecurity Of Federal Networks And Critical Infrastructure*[3]. This order requires that "…each agency head shall use The Framework … to manage the agency's cybersecurity risk."

While the Federal government has long relied on NIST guidance to manage risk, this latest step moves the government towards a more general alignment with the private sector, who is instrumental in the development of the Framework and is currently adopting it at a significant rate.

[3] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

Combined with the Administration's push to modernize government information technology[4], there is tremendous opportunity for innovative technology developers and vendors to bring solutions that help agencies meet policy goals while dramatically improving their security posture.

How organizations use the NIST Framework

The NIST Cybersecurity Framework[5] has proven to be a valuable tool in many ways, including enabling cybersecurity personnel to identify and report risks, needs, and accomplishments to senior leaders in a way that is both relatively easy to understand and broadly recognized. This in turn allows leaders to make informed and more defensible decisions, even at the board level.

But the Framework is only as good as the people, processes, and technology that support it. The ability to communicate and manage a cybersecurity program effectively is dependent on personnel understanding how technology solutions will align with the Framework in a way that allows them to build a comprehensive risk management picture across the enterprise.

To assist with this, product vendors across the information technology (IT) and cybersecurity industries are looking at how customers can implement their products and services in support of Framework-based risk management and reporting. For senior leaders looking to understand their organization's cybersecurity risk and how it can be managed in practical terms, this is a powerful approach. It takes what can be complex concepts and terminology and breaks them down in ways that can be tied to budgets and resources, without losing the important granularity needed by implementers and operators to be successful.

[4] https://www.whitehouse.gov/blog/2017/08/30/it-modernization
[5] https://www.nist.gov/cyberframework

APPENDIX B: ANALYSIS MATRIX

	ID	Description	Support	Capability	Rationale
IDENTIFY					
	ID.AM-3	Organizational communication and data flows are mapped.	INFORM	Governance	SailPoint shows the relationships between users, systems, and data. This is an important aspect of understanding how communications and data move around the organization.
	ID.AM-5	Resources are prioritized based on their classification, criticality, and business value.	INFORM	Governance	SailPoint provided significant insight tied to users and assets that aids in prioritization.
	ID.BE-4	Dependencies and critical functions for delivery of critical services are established.	INFORM	Governance	Analysis of user behavior can reveal critical data sets or systems based on frequency and/or type of access.
	ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	INFORM	Governance	The role-based approach taken by the SailPoint platform ensures that internal roles and responsibilities are understood and authorized in a manner that highlights gaps and enables needed changes to be more easily identified.

	ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	CONTRIBUTE	Governance	Identity and credential management are foundational elements of many regulatory and contractual requirements. The SailPoint Governance Platform contributes directly to being able to meet these requirements by enabling organizations to understand and manage these requirements and report directly on compliance with those elements.
PROTECT	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	COMPLETE	Access Control	This is a core capability of what SailPoint provides.
	PR.AC-2	Physical access to assets is managed and protected.	INFORM	Access Control	To the extent that physical access controls are integrated with logical systems, SailPoint can manage access to those assets.
	PR.AC-3	Remote access is managed.	CONTRIBUTE	Access Control	Access controls can be assigned for remote employees to include connectivity/authentication and device requirements.
	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	COMPLETE	Governance	This is a core capability of what SailPoint provides.
	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions.	CONTRIBUTE	Governance	SailPoint relies on some external function, such as HR, for original proofing, but does the rest.

PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	CONTRIBUTE	Access Control	The Sailpoint Governance Platform provides insight on which users are on the network and what they have access to. This is not specifically "authentication" as defined in this Subcategory, but clearly contributes to the overall management.
PR.DS-1	Data-at-rest is protected.	CONTRIBUTE	Access Control	SailPoint contributes to protecting data by streamlining the review of access controls on a per-user basis, ensuring that administrators can limit access to the least number of users possible.
PR.DS-2	Data-in-transit is protected.	CONTRIBUTE	Access Control	SailPoint contributes to protecting data by streamlining the review of access controls on a per-user basis, ensuring that administrators can limit access to the least number of users possible.
PR.DS-3	Assets are formally managed throughout removal, transfers and disposition.	CONTRIBUTE	Governance	Asset management is tied to user access and interaction. As a result, SailPoint contributes directly.
PR.DS-5	Protections against data leaks are implemented.	CONTRIBUTE	Access Control	Through managed access control and user monitoring, the likelihood of unauthorized transfer of data is reduced.

				Credential management is essential to ensuring that users are limited to appropriate network boundaries, such as those between development and production environments. SailPoint provides that insight, enabling administrators to implement and maintain those restrictions effectively.
PR.DS-7	The development and testing environment(s) are separate from the production environment.	CONTRIBUTE	Governance	
PR.IP-8	Effectiveness of protection technologies is shared.	INFORM	Analytics	SailPoint's reporting capabilities can be a useful addition to the reporting done across all protection technologies.
				The provisioning and de-provisioning of user credentials is an essential function of human resource management. Regardless of where the actual activity takes place, SailPoint provides the necessary capabilities to ensure users are added to or removed from the network in a timely manner.
PR.IP-11	Cybersecurity is included in human resources practices (e.g. deprovisioning, personnel screening).	CONTRIBUTE	Access Control	
PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.	CONTRIBUTE	Access Control	SailPoint can manage remote maintenance of assets (e.g. helpdesk).
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	CONTRIBUTE	Access Control	SailPoint provides the necessary oversight and control into who has access to assets to ensure that only authorized users are

					permitted to conduct maintenance activities.
	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	CONTRIBUTE	Analytics	SailPoint contributes its information into the organizations overall audit/log records.
	PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	CONTRIBUTE	Access Control	User access control includes the ability to limit what users can do with any given asset.
	PR.PT-4	Communications and control networks are protected.	CONTRIBUTE	Access Control	Communication and control networks require careful provisioning of users and their access, which SailPoint contributes to directly.
DETECT	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.	CONTRIBUTE	Governance	SailPoint contributes directly to the development of a baseline regarding user access, which in turn is a core element in the overall baseline of network operations and data flow.
	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.	CONTRIBUTE	Analytics	SailPoint contributes to the overall event data that can be collected and analyzed.
	DE.AE-4	Impact of events is determined.	CONTRIBUTE	Analytics	SailPoint's insight into user access can aid in determining the impact of certain kinds of incidents, particularly those involving a compromised user credential.
	DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events.	CONTRIBUTE	Analytics	While not directly monitoring user events, SailPoint's governance capabilities provides the

					foundation for ensuring that users are only permitted access to appropriate assets and can alert when they have attempted to violate a restriction.
	DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events.	CONTRIBUTE	Analytics	As with DE.CM-3 above, accounts of external service providers can be managed and monitored.
	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.	CONTRIBUTE	Analytics	Unauthorized personnel, or authorized personnel performing unauthorized actions, would be flagged by SailPoint.
RESPOND	RS.CO-2	Events are reported consistent with established criteria.	INFORM	Analytics	SailPoint provides alerts and information related to identity governance that informs the overall event management processes.
	RS.AN-1	Notifications from detection systems are investigated.	CONTRIBUTE	Analytics	SailPoint events can be sent to detection systems, and its own events can be investigated.
	RS.AN-2	The impact of the incident is understood.	INFORM	Analytics	SailPoint enables the rapid understanding of user accounts that may be compromised or otherwise implicated in an incident.

RS.AN-3	Forensics are performed.	CONTRIBUTE	Analytics	SailPoint's analytics capabilities can assist in reconstructing possible root causes for an incident through discovering rogue users and/or compromised accounts.
RS.MI-1	Incidents are contained.	CONTRIBUTE	Access Control	SailPoint enables the de-provisioning of account and restriction of access, thereby giving administrator and network defenders an additional tool in dealing compromised user account.
RS.MI-2	Incidents are mitigated.	CONTRIBUTE	Access Control	SailPoint enables the de-provisioning of account and restriction of access, thereby giving administrator and network defenders an additional tool in dealing compromised user account.